Japanese Unexamined Patent Publication (kokai). No. 62-256046

(43) Date of Publication: November 7, 1987

(21) Application Number: 99581/1986

(22) Date of Filing: April 30, 1986

(71) Applicant: Ricoh Co., Ltd.

(72) Inventor: Tsunetada IZUMI and Shinichiro AIMI

STRUCTURE

In order to achieve the above object, the present invention offers a capability in which security protection can be set in the unit of character.

Hereinafter, detailed description will be given based on an embodiment of the present invention.

Fig. 2 is a perspective view of an overall appearance of a word-processing and communication terminal as an information processing apparatus according to an embodiment of the present invention.

The word processing and communication terminal comprises: a keyboard 1 which includes keys representing katakana, hiragana, Chinese characters, Roman alphabet, Arabic figures (translator's comment: "katakana" and "hiragana" are two types of Japanese alphabet), necessary for inputting character data and control data used in word processing, document transmission and system control; a display 2 which displays document data as well as control information necessary for various operations such as document creation and edition operations and document transmitting operation; a wire-dot serial printer 3 for recording on recording paper such information as a

document created by the word processing system, a document received from elsewhere, transmission record, reception record and so on; a main body 4 including therein a floppy disc drive and a thin-type hard disk drive, a system control unit, a communication control unit as a communication controlling apparatus, and so on; a mouse 5; and a telephone 6.

The word processing and communication terminal has a teletex communication and a facsimile communication capabilities in conformity with the CCITT Recommendation on Telex and Facsimile Communications and the Recommended Method of Communications in Japanese-Language Teletex System announced by the Japanese Ministry of Posts and Telecommunications.

Fig. 3 is a block diagram of an inner configuration of the main body 4.

The hard disk drive (HDD) 7 is provided for example, by a 20 megabyte hard disk drive unit (HDD), which stores an operating system (OS) capable of resident processing function for multi-task operation, as well as a conversion program between Japanese characters and Chinese characters, a conversion dictionary between Japanese characters and Chinese characters, document data under processing, a document transmission-and-reception program, and so on.

The floppy disc drive (FDD) 8 is provided by a known 5-inch, double-density floppy disk drive (FDD), and stores document data and other information.

The system control unit (SCU) 9 provides overall control of the entire terminal, and performs word processing procedures for document creation and edition, procedures related to data compression processes for document to be transmitted, procedures related to document transmission and reception to and

from the communication control unit 11, and local transmission and reception procedures including printing of a received document.

A CRT control unit (CRTCU) 10 controls displaying in the display 2 and printing in the printer 3.

The communication control unit (CCU) 11 is provided by a communication control apparatus, and controls communications with a counterpart terminal such as a teletex terminal, a facsimile machine (FAX), or another terminal of this model of word processing and communication terminal.

A data compressing unit (DCR) 12 converts an image data to a set of compression codes in accordance with the facsimile communication standards.

Though not illustrated, the main body 4 also includes a mouse interface for the mouse 5, a scanner interface for a scanner, and so on.

Fig. 4 is a block diagram of an example of the system control unit 9.

The system control unit 9 includes: a CPU 21 provided primarily by a 16-bit microprocessor which takes an overall control of the entire system; a bus buffer 22 placed between the CPU 21 and a common bus, a timing generator 23 and a refresh controller 24.

Further, the system control unit 9 includes: a RAM 25 having a memory capacity of e.g. 512 kB which provides a system memory region resided by the OS and other residual programs such as one related to document reception, and other memory regions; RAM controllers 26 and 27 which control the RAM 25; and a boot ROM 28 which stores a boot program for conducting a program loading from the HDD 7 to the RAM 25 when the powder supply is turned on.

Further, the system control unit 9 includes: a keyboard interface (I/F) 30 which controls information transmission with the key board 1; a hard disk

interface (HDDI/F) 31 which controls the HDD 7; a buffer 32 placed between the HDDI/F 31 and the common bus; and a floppy disc controller (FDC) 33 which controls the FDD 8.

Still further, the system control unit 9 includes serial ports (SIO) 34 and 35.

Fig. 5 is a block diagram of an example of the CRTCU 10.

The CRTCU 10 includes: a slave CPU 41 provided primarily by a 16-bit microprocessor which takes overall control; a bus I/F 42 placed between a slave CPU bus and the common bus; a ROM 43 having a memory capacity of e.g. 16 kB for IPL; and a RAM 44 which provides a program memory and a shared memory shared with the system control unit 9.

The shared memory provided by the RAM 44 includes an index buffer, a management memory region, a recording memory region, data buffer for FAX transmission, a page buffer for the printer, and a data buffer for image edition.

Further, the CRTCU10 includes a bus I/F 45 placed between the slave CPU bus and a microbus, a ROM 46 for micro-programs, and a RAM 47 for program control memory.

Further, the CRTCU 10 includes: a character graphic (CG) memory 48 provided by a ROM for Chinese character patterns, a ROM for layout data, a ROM for the system, and a RAM for user-defined character patterns; and a CRT controller 49.

Still further, the CRTCU 10 includes: an image memory 51 which develops a data to be displayed on the display (CRT) 2; a timing generation circuit 52 which controls display timing; and a printer I/F 53 which controls data transmission with the printer 3.

Fig. 6 is a block diagram of an example of the communication control unit (CCU) 11.

The communication control unit 11 includes: a CPU 61 provided primarily by a 16-bit microprocessor which takes overall control; a parallel interface 62 with the common bus; a ROM 63 which stores control programs for teletex communication and facsimile communication; a RAM 64 serving mainly as a working memory; and a RAM 65 used as a communications memory for storing document data received, document data to be transmitted, and transmission/reception log data, for performing inter-memory communications.

Further, the communication control unit 11 includes the following components in order to perform communication with a counterpart terminal via a public telephone link: a multi-protocol serial control (MPSC) 66; a modem 67; a line interface 68; a telephone-link controller (AA-NCU) 69; a terminal 70, a telephone-line protection device (PD) 71 and a modem 67; a modem interface 72; and an NCU interface 73 for the telephone-line controller 69.

Further, the communication control unit 11 includes a calendar 74 used for date management and other purposes, switches (LP/SW) 75 for internal settings, an indicator interface 76, and an LED indicator 77 for indicating reception of a document for example.

Though not illustrated, the communication control unit 11 also includes an X.21 interface and a connector which allow access to a packet communication network and other communication networks, in addition to the public telephone link.

Fig. 7 is a block diagram of an example of a DCR 12.

The DCR 12 controls the entire system through a microcomputer

system provided by a CPU 81, a ROM 82 and a local RAM 83.

A shared memory 84 is a memory shared by the DCR 12 and the system control unit 9 (host), and includes a command response area for storing commands and responses, an image data area for storing an image data (picture data) to be compressed, and a compression code area for storing the compressed image data (picture data).

An FCP (facsimile control processor) 85 compresses the image data stored in the image data area of the shared memory 84, and write the compression codes (picture data) after the compression, in the compression code area of the shared memory 84.

A data inversion gate 86 allows a data to be written in the shared memory 84 or a data read out of the shared memory 84 to pass through in the reverse (inverted) order of the original bits. A data non-inversion gate 87 allows the data to be written in the shared memory 84 or the data read out of the shared memory 84 to pass through in the original order of the bits.

An address decoder 88 decodes an address data from the common bus, and outputs such information as gate request AREQ which selects the data inversion gate 86, gate request BREQ which selects the data non-inversion gate 87, as well as host request HOST, register select REGSL, and card select CSL which compose a request for use of the shared memory by the host.

A selector 89 selectively switches a data input-output line to and from the shared memory, to one of the FCP 85, the data inversion gate 86 and the data non-inversion gate 87, as well as outputting Out-Enable OE or Write-Enable WE to the shared memory 84, and outputting a bus flag BUSFALG.

An address decoder 90 outputs Shared Memory Select C-RAMSL and

FCP Select FCPSL to the FCP 85 in accordance with an address data from the CPU 81, and outputs ROM Select ROMSL to the ROM 82 and Local RAM Select RRAMSL to a local RAM 81.

In addition to the above, the DCR 12 includes a command status register 91, an interruption flag 92 and so on.

Fig. 1 is a block diagram of a functional relationship among portions of the terminal which are related to the security control.

An inputting unit 101 inputs character codes, control codes necessary for creation and edition of a document, and control codes necessary for transmission of the document. A security specifying unit 102 inputs a direction specifying a character to be held under security in the document. A security level specifying unit 103 inputs a level of security specified to the confidential character. These units correspond to the keys in the keyboard 1.

An input checking unit 104 checks if the information inputted from the inputting unit 101, the security specifying unit 102 and the security level specifying unit 103 is a character code, a word processing control code, security specifying code, security level specifying code, transmission controlling information, password or otherwise, and depending on the type of the information, forwards the inputted information to a relevant unit. The input checking unit 104 corresponds to the input control unit of the system control unit 7.

A display unit 105 displays document data and so on, a printing unit 106 prints the document data and so on, and an output control unit 107 controls the display unit 105 and the printing unit 106. These correspond to the CRT display 2, the printer 3 and the CRTCU 10 respectively.

An external storage unit 108 stores document data, co-system programs and so on. An external storage controls unit 109 controls writing and reading of information to and from the external storage unit 108. These correspond to the hard disk drive 7, the floppy disc drive 8, and the HDDI/F 31 and FDC 33 in the system control unit 9, respectively.

A communication control unit 110 controls teletex communication and facsimile communication with respective counterpart terminals, and thus corresponds to the communication control unit 11.

A document creation/edition unit 111 receives the character code, the word processing/edition control code, the security specifying code and the security level specifying code inputted via the input checking unit 104, thereby creating and edition the document, having the display unit 105 display the edited document via the output control unit 107, storing or reading the document in and out of the external storage unit 108 via the external storage control unit 109.

Further, when a security protection setting code is inputted, the document creation/edition unit 111 adds a security protection starting code and security protection ending code to respective characters specified. Likewise, when security level code is inputted, the unit adds security level code to the confidential data.

Further, if a document read out of the external storage unit 108 contains a password (a unique character string), then the document creation/edition unit 111 calls a password control unit 112 for comparison of the registered password with an inputted password.

Still further, when requested to read a received document stored in the

external storage unit 108, the document creation/edition unit 111 calls a confidential data detector unit 113, a security level detector unit 114 and a level checker unit 115, in order to determine if the read character data is authorized for outputting, and performs output control of the character data in accordance with the given determination.

Upon reception of the password comparison command from the document creation/edition unit 111, the password control unit 112 controls the external storage control unit 109, reads a document password file, extracts the password registered for the given document, calls the display unit 105 for displaying an "Enter password" prompt via the output control unit 107, then compares the password entered via the inputting unit 101 and the input checking unit 104, with the registered password, and sends a result of the comparison to the document creation/edition unit 111.

A confidential data detector unit 113 checks if data sent from the document creation/edition unit 111 is a confidential data or not, and if the data is confidential, notifies it to a security level detector unit 114. Upon notice from the confidential data detector unit 113, the security level detector unit 114 detects the security level code, and send this data to the level checker unit 115. The level checker unit 115 compares the level data sent from the security level detector unit 114 with a security level specified to the terminal which is a predetermined information stored in a level memory 116 in the terminal. A result of the comparison is sent to the document creation/edition unit 111.

When a transmission command is sent from the inputting unit 101 via the input checking unit 104, a local transmission/reception control unit 117 controls the external storage unit 109, loads a specified transmission document

from the external storage unit 108, and sends the document to the communication control unit 110. Likewise, the local transmission/reception control unit controls the external storage unit 109, and stores a received document sent from the communication control unit 110, in the external storage unit 108.

Next, functions of the embodiment configured as mentioned above will be described, with reference to Fig. 8 and the following drawings.

First, description will cover a document transmission process in the present word processor and communication terminal, with reference to Fig. 8.

When document transmission is selected in a telex communications menu, in an unillustrated task selection process, a transmission condition setting process is performed first, in which the process displays a document transmission preparation menu on the display, and receives from the keyboard such data as transmission mode (normal transmission, emergency transmission, etc.), transmission time of the day, and content of the document (a document in Japanese, etc.).

After completing the transmission condition setting process, a document selection process is performed, in which the process reads titles of documents registered in a document file, displays a menu which is a list of the documents from which a transmission document is to be selected, and when the selection is made via the keyboard, the selected document is loaded.

After completing the document selection process, an address selection process is performed, in which the process reads a registered address list from an address file, displays an address selection menu, and when the selection is made via the keyboard, the selected address is loaded.

After completing the address selection process, a display is made for confirmation of the selected address, title of the document, and so on. If cancellation is selected, the process goes to perform a cancellation process, whereas if confirmation is selected, the process goes to perform a transmission preparation process to be described below.

In the transmission preparation process, the system control unit (SCU) 9 first forwards transmission information including a specified address (dial number), document title, transmission time of the day, etc. to the communication control unit 11.

On the other hand, the communication control unit (CCU) 11 begins to perform a process shown in Fig. 9 upon reception of a predetermined command from SCU 9, and receives the transmission information forwarded from the SCU 9.

If CCU 11 is unable to receive information from SCU 9, due to another document transmission task, for example, then this preparation process, including data exchange of the transmission information with SCU 9, is put on hold until the ongoing transmission is finished.

Thereafter, SCU 9 checks a transmission mode registered in the address list or newly specified via the keyboard, to see if the transmission is to be made via facsimile (FAX) or teletex (TELETEX).

If the transmission mode is the FAX mode, then CCU 11 is requested to supply a file number, and upon the request, CCU 11 sends out an appropriate file number. The file number has a predetermined format, such as "TDOC-xxx" for the Teletex mode, and serves for internal management.

Next, SCU 9 converts the file number sent by CCU 11, from the Teletex

format, i.e. "TDOC-xxx" to a FAX format, e.g. "FDOC-xxx".

Then, SCU 9 reads the specified transmission document from FDD 8, attaches the converted file number "FDOC-xxx" to the document, stores the document in a transmission file provided by HDD 7, and sends the converted file number to CCU 11.

On the contrary, if the transmission mode is not the FAX mode, i.e. if the transmission mode is the Teletex mode, then similar steps follow. In detail, CCU 11 is requested to give a file number.

Next, the file number received from CCU 11, i.e. "TDOC-xxx" of the Teletex format, is attached to the document, without conversion, and the transmitted document is stored in the transmission file.

It should be noted here that upon reception of the converted file number from SCU 9, CCU 11 changes the file number which was sent to SCU 9 to the converted file number received from SCU 9, and registers this new file number.

Next, a transmission process performed by the system control unit 9 and the communication control unit 11 will be described with reference to Figs. 10 and 11.

When a specified transmission commencing time of the day is reached, or if nothing is specified on the transmission commencing time, the communication control unit (CCU) 11 immediately determines that it should start the transmission, and sets a transmission status (issues a transmission command).

Meanwhile, the system control unit (SCU) 9 poles CCU 11 at a predetermined time interval to see if the transmission status is set, and when the transmission status is set, i.e. when the transmission command has been

received, SCU requests CCU 11 for the file number (transmission file number).

On the other hand, upon reception of the request for the transmission file number, CCU 11 sends the transmission file number to SCU 9, and waits for a command from SCU 9.

Then, SCU 9 checks if the transmission file number received from the CCU 11 is of the "TDOC-xxx" format or of the "FDOC-xxx" format, to determine if the transmission is to be made in the FAX mode.

If the transmission file number is of the FAX mode format, a FAX document transmission command is sent to CCU 11, whereas if the transmission file number is of the TELETEX mode format, a TELETEX document transmission command is sent.

CCU 11 checks if the command received from SCU 9 is a FAX transmission command or not, and depending on the command, follows the facsimile transmission standards or the teletex transmission standards to perform a communication link connecting process with the addressee (counterpart).

When the communication link is established and is ready for transmission, a transmission document sending process and a transmission document reception process are performed between SCU 9 and CCU 11, in accordance with the selected transmission mode (FAX/TELETEX).

Thereafter, CCU 11 transmits the transmission document data received from SCU 9 to the addressee, in accordance with the transmission mode (FAX/TELETEX).

SCU 9, upon completion of the transmission of the transmission document to CCU 11, or in case the transmission is disabled, performs a

transmission ending process, whereas CCU 11, upon completion of its transmission of the transmission document to the addressee, or in case the communication link is disabled, performs a transmission ending process, to complete the entire sequence of the processes.

Next, an example of document creation process will be described with reference to Fig. 12.

The document creation process begins with a stand-by step waiting an input from the keyboard 1. Upon input from the keyboard 1, the process checks if the key-input represents a character or not.

If the key-input is a character, the process stores the inputted character code at an address in the document edition area indicated by a write pointer, displays the inputted character on the CRT display 2, and then returns to the stand-by step waiting for a new key-input 1.

If the input through the key is not a character, the process checks whether or not the input is a security setting command issued via a specific key or via a combination of keys provided in the keyboard.

If the input is a security set command, the process stores a "security mode set code", which is a predetermined data representing a starting point of confidential information, at an address of the document edition area indicated by the writing pointer.

Then, the process displays a string of characters on the CRT display 2, prompting for an input of a code for setting the security level (hereinafter called document security level) to be specified to the confidential character. The security level code inputted through the keyboard 1 is then stored at an address of the document edition area indicated by the writing pointer.

It is to be noted here that in the above setting of the security level, a menu is displayed, so the selection is made from such options as: setting of a new security level, continued use of the current security level specified in the previous setting, and use of default security level predetermined for the terminal. Depending on the selection, the corresponding security level code is identified from a security code inputted through the keyboard 1, a security code stored in the previous setting and a security code defined for the terminal, and then the identified level code is stored.

Further, the document security level can have 256 grades from "0 - 255" for example, with the security level "0" being the highest security level. Further, the security level for the terminal can also have 256 grades from "0 - 255", with the security level "0" being the highest security level. The terminal security level is set at the time of system generation. Alternatively however, the terminal security level may be set by a combination of security level setting switches.

Thereafter, the process goes back to the stand-by step to wait for a new key input, and upon key input, the process checks if the input is a security protection end command with a specific key or through a combination of keys provided in the keyboard 1.

If the input is not the security protection end command, the process checks if the input is a character or not. If the input through the key is a character, the process stores the inputted character code at an address of the document edition area indicated by the writing pointer, displays the character, and then returns to the stand-by step waiting for a new key input. If the input is not a character, then the process performs a procedure relevant to the key

input, and then returns to the stand-by step waiting for a new key input.

If the key-input is the security protection end command with the specific key(s), the process stores a "security mode reset code", which is a predetermined data representing an ending point of confidential information, at an address of the document edition area indicated by the writing pointer, and then returns to the stand-by step waiting for a new key input.

Further, if the key-input is not the security protection end command made through the specific key(s), the process checks if the input is from an "end of edition" key. If the input is from the "end of edition" key, the process stores a title of the document currently being edited, and then stores a password set for the document. It should be noted that the setting of password to a documents is an arbitrary selectable option. Finally, the document is stored in the floppy disc drive 8.

Next, another example of document creation process will be described with reference to Fig. 13.

According to this document creation process, when there is an input from the keyboard 1, and if the process has determined that the input is a confidential mode command from a specific key or from a combination of keys provided in the keyboard 1, the process stores the "security mode set code" at an address of the document edition area indicated by the writing pointer.

Then, the process performs the security level setting process, in the same way as in the above-described document creation process, and then moves a cursor to a position specified by a "move cursor command" received from the keyboard 1. This cursor moving process is repeated until an "execution" key provided in the keyboard 1 is pressed.

When the execution key is pressed, the process stores the "security mode reset code" at an address of the document edition area indicated by the writing pointer, and then substitutes a character string sandwiched by the "security mode set code" and the "security mode reset code", with a string of a predetermined dummy character (such as a space, a shade, and any other predetermined character), and displays the substituted character string, on the display.

Other processes are the same as those described in the previous document creation process.

Now, these document creation processes will be described in an example, with reference to Figs. 14 and 15.

The description will cover an example, in which a document shown in Fig. 14(A) is newly created, and security protection will be set for a figure "100" included in a Japanese phrase "原価：１００万". (Translator's comment: In the Japanese phrase, 原価 means "cost", and 万 means "ten thousands".)

As a first case, the process shown in Fig. 12 will be followed. Specifically, a key-input will be continued until the phrase "原価： (cost:)" has been entered. Then, by pressing a security protection start key, a security protection set command is inputted. Specifically, as shown in Fig. 15, the "security mode set code" (indicated by "モードON (ON MODE)") is stored at an address next to the "原価 (cost)": in the document edition area. Then, when the security level (document security level) is set, a document security level code (indicated by "文書レベル(document level)") is stored at an address next to the "モードON (ON MODE)".

Thereafter, the figure "100" is inputted, and the characters of "100" are

stored respectively at addresses following the "document level". Then, by pressing a security protection end key, a security protection end command is inputted. Namely, the "security mode reset code" (indicated by "モード OFF (OFF MODE)") is stored at an address next to "100". Then, when the key-input is received for the character "万 (ten thousands)", the character representing the "ten thousands" is stored at an address following the "OFF MODE".

In this way, the confidential word "100" is sandwiched by the "security mode set code" and the "security mode reset code", and this character string is registered as a confidential part. In other words, according to this document creation process, the confidential part is set during the character inputting operation.

Next, the process shown in Fig. 12 will be followed. According to this process, key-input is continued until the phrase "原価：１００万 (cost: 1,000 thousands)" has been inputted. Then, the cursor is moved back onto "1" of the figure "100", and by pressing the security protection start key, as in the above-mentioned case, a "security mode set code" is inserted and stored. Then, when the security level is set, a document security level code is stored at the next address.

Thereafter, the cursor is moved onto the last character "0" and the execution key is pressed, whereupon the "security mode reset code" is inserted after this character "0", and the figure "100" on the display changes to a dummy character string (e.g. a shadow space) as shown in Fig. 14(B). In other words, unlike the above-mentioned document creation process, according to this document creation process, the confidential part is set after the document is created. In addition, after the security is set, display of the specified character

string is substituted by a dummy character string. This offers an advantage that confidential information is protected from other person's eyes even during the document creation.

It should be noted here that the above two kinds of document creation processes can be used in combination. Specifically, in one mode, the security can be set when inputting characters, and the confidential character string is displayed as a dummy character string, whereas in another mode, the security is set after inputting characters, and the confidential character string is not substituted by the dummy character string till the end of the document creation.

Next, a registered-document outputting process will be described with reference to Fig. 16. The registered-document outputting process is performed for example, when a document is updated, printed and so on.

According to the registered-document outputting process, first, the title of a document to be loaded is entered. The process checks if there is a registered document identified by the entered title. If the document is found in the registration, the process further checks if the document is a received document or not. Whether or not the document is a received one can be checked for example by comparing the title of the registered document with titles of received documents stored in the file of received documents.

If the document to be loaded is not a received document, then the process further checks if there is a password set for the document, by checking for example a file of document passwords which stores passwords set for each of the documents.

If there is a password set, the process displays on the CRT display 2 a

prompt which requests inputting of a password, and the inputted password is then checked against the valid password registered for the document.

If the inputted password is identical with the registered password, or if no password is set to the document, the process performs the document outputting process, in which the specified document is read out of the document file, and outputted (i.e. displayed or printed).

In other words, even if security is set to a document when the document is created, if no password is set for the document, or if a valid password is entered, then the security setting is unlocked and the entire contents of the document is outputted. With this arrangement, even if security is set to a document, the author of the document can output the entire content of the document.

On the other hand, if the document to be read out is a received document, or if a valid password is not entered for a document which is not a received document but locked with a password, then the process first loads the specified document onto the internal memory.

Then, the process reads out data from this document, and checks if the data is the "security mode set code". If the data is the "security mode set code", the process further reads the next data, which is the security level code, and checks if the document security level specified for this document is higher than the terminal security level specified for this terminal (document > terminal). If the document security level is higher than the terminal security level, then the process sets security mode flag F to 1, i.e. F=1.

On the other hand, if the read data is not the "security mode set code", the process checks if the data is the "security mode reset code". If the data is

the "security mode reset code", then the process resets the security mode flag F to a value "0".

Further, if the read data is not the "security mode reset code", the process checks if the data is a character data. If the data is a character data, then the process checks the security mode flag F to see if the value of F is one or not, i.e. to see if the character data is set to the security mode and the specified security level is higher than the terminal security level. If the security mode flag F = 1, which means this character string is not allowed to be outputted, then the process outputs a predetermined dummy character string. On the other hand, if the security mode flag F = 0, the process outputs this character string.

Still further, if the read data is not a character data, the process performs a process relevant to this data.

After performing one of the above described processes, the process checks if the end of the document is reached, and continues the above described cycle of processes until the end of the document is reached.

Therefore, if a document is received and the document is such a one as shown in Fig. 14 locked with security setting as described above, all the characters contained in the document but before the phrase "原価 : (cost:)" are outputted. However, when the next data is read out, the data is the "security mode set code" (ON MODE). Thus, the process further read out next data, which is the "security level code", and if the document security level is higher than the terminal security level, then the process sets the security mode flag F to 1.

With this setting, then the process further reads the next data, which is

a character data "1", and since the current security mode flag F = 1, the process does not display this particular character "1" but displays a dummy character (such as a shaded space). The process performs the same procedure for the following characters "0" and "0" and displays the dummy characters.

Then, when the process reads the next data, the data is the "security mode reset code" (OFF MODE). The process then resets the security mode flag F = 0, and thus, when the next data is read, the data, which is the character "万 (ten thousands)" is displayed.

In this way, when the document is a received document, any character string sandwiched between the "security mode set code" and the "security mode reset code" is not displayed if the document security level is higher than the terminal security level. This provides security protection. Further, even if the document is not a received document, since the character string locked with the security setting is not accessible by edit function, no one but the original author can change the content, and therefore security is protected.

As has been described, according to the present word processing and communication terminal, security setting can be set for each character, on a character-by-character basis. This improves document usability. Further, this makes possible to transmit a document partially masked for security, which improves document usability at the receiving end.

Further, according to the conventional word processing and communication terminal, when transmitting a document which is partially confidential, a specific masking operation must be performed depending on a security level set to the receiving end, in order to actually mask the confidential part with a string of spaces, shades etc., before the document can be

transmitted. This process is laborious, and in addition, even if the same document is to be transmitted to a plurality of terminals, different levels of masking operation must be performed corresponding to the different levels of the receiving ends, which makes it difficult to use a broadcast communication apparatus.

On the contrary, according to the present word processing and communication terminal, by enabling the security protection to be specified on a character-by-character basis, and by adding information indicating the level of security, only one document can serve all transmissions to a plurality of terminals having different levels of security setting. This allows the use of the broadcast communication apparatus, making easy the document transmission.

It should be noted here that according to the above embodiment, the present invention is applied to a word processing and communication terminal. Alternatively, the present invention can also be applied to a standalone word processor, data processor and other information processing apparatus which do not have a transmission capability.

Further, according to the above embodiment, description is made for cases in which a confidential document is transmitted without an attachment of the password. Alternatively, the terminal may have a capability to attach a password to a transmitted document so that the security setting can be unlocked at the receiving end by entering the password. The transmission of the password can be performed in accordance with CCITT Recommendation S.62, Session in End-to-End Control Procedure, or Private Parameter stipulated in the Document Control Procedure, for example.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭62-256046

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和62年(1987)11月7日
G 06 F 11/00	340	7368-5B	
G 09 C 1/00		7368-5B	

審査請求　未請求　発明の数 1　(全16頁)

⑤4発明の名称　情報処理装置

⑳特　願　昭61-99581
㉒出　願　昭61(1986)4月30日

⑦2発明者　泉　経忠　東京都大田区中馬込1丁目3番6号　株式会社リコー内
⑦2発明者　会見　真一郎　東京都大田区中馬込1丁目3番6号　株式会社リコー内
⑦1出願人　株式会社リコー　東京都大田区中馬込1丁目3番6号
⑦4代理人　弁理士　大澤　敬　外1名

明　細　書

1.発明の名称

情報処理装置

2.特許請求の範囲

1　機密設定を指示する機密指示手段と、該機密指示手段の指示結果に応じて文字単位で機密開始情報及び機密終了情報を付加する機密範囲設定手段と、該機密範囲設定手段の設定結果に応じて出力制御をする出力制御手段とを備えたことを特徴とする情報処理装置。

2　機密範囲設定手段が設定した機密範囲の機密レベルを設定する手段をも備え、出力制御手段が受信文書に設定されている機密範囲の機密レベルと予め定めた装置の機密レベルとに応じて受信文書の出力制御をする手段をも備えている特許請求の範囲第1項記載の情報処理装置。

3.発明の詳細な説明

技術分野

この発明は、情報処理装置に関し、特に機密保護に関する。

従来技術

一般に、オフィスコンピュータ，パーソナルコンピュータ，ワードプロセッサ，データプロセッサあるいはコミュケーションワードプロセッサ，テレテックス等の各種の情報処理装置においては、文書等の機密保護が重要になつてきている。

ところが、従来の情報処理装置としての例えば文書作成編集装置においては、文書自体にパスワード（暗証）を付加することによつて機密保護をするようにしている。

そのため、文書のすべての情報について機密保護の必要がない場合でも、機密が設定された文書は所有者や以外の者がまつたく使用することができなくなるという不都合がある。

目　的

この発明は上記の点に鑑みてなされたものであり、機密保護が必要な文書等の利用性を向上することを目的とする。

構　成

この発明は上記の目的を達成するために、文字

単位で機密範囲を設定する機能を備えたものである。

以下、この発明の一実施例に基づいて具体的に説明する。

第２図はこの発明を実施した情報処理装置としての文書作成通信端末装置の一例を示す外観斜視図である。

この文書作成通信端末装置は、文書作成，文書伝送及びシステム制御に必要な片仮名，平仮名，漢字，英字，数字等の文字情報及び制御情報を入力するためのキーを有するキーボード１と、文書作成編集操作及び文書送信操作等の各種操作に必要な情報や文書情報を表示するディスプレイ装置２と、作成文書情報や受信文書情報並びに送信記録，受信記録等を記録紙に記録するワイヤドットシリアルプリンタ３と、フロッピディスク装置及び薄型ハードディスク装置，システム制御部，通信制御装置としての通信制御部等を内蔵した本体４と、マウス５及び電話６とを備えている。

なお、この文書作成通信端末装置におけるテレテックス通信及びファクシミリ通信に関する仕様は、テレテックス及びファクシミリに関するＣＣＩＴＴ勧告並びに郵政省告示の日本語テレテックス装置推奨通信方式に準拠する。

第３図は本体４の内部構成を示すブロック図である。

ハードディスクドライブ装置（ＨＤＤ）７は、例えば２０メガバイトの容量を有するハードディスクドライブ装置（ＨＤＤ）からなり、マルチタスク制御が可能なレジデント（常駐）プロセス機能を有するオペレーティングシステム(ＯＳ)，かな漢字変換プログラム，かな漢字変換辞書，作成文書情報，文書送受信プログラム等を格納する。

フロッピディスクドライブ装置（ＦＤＤ）８は、公知の５インチ・ダブルデンシティ・フロッピディスクドライブ装置（ＦＤＤ）からなり、文書情報等を格納する。

システム制御部（システム・コントロール・ユニット：ＳＣＵ）９は、この端末装置全体の制御を司り、文書の作成編集等のワードプロセッシング処理及び送信文書のデータ圧縮処理並びに通信制御部１１との間の文書送受信に係わる手順，受信文書印字などのローカル送受信処理を実行する。

ＣＲＴ制御部（ＣＲＴ・コントロール・ユニット：ＣＲＴＣＵ）１０は、ディスプレイ装置２の表示制御及びプリンタ３の印刷制御を司る。

通信制御部（コミニケーション・コントロール・ユニット：ＣＣＵ）１１は、通信制御装置であり、テレテックス端末装置，ファクシミリ装置（ＦＡＸ）及び同機種の文書作成通信端末装置等の相手先端末装置に対する文書の送信制御並びに相手先端末装置からの文書の受信制御等の通信制御を司る。

データ圧縮部（ＤＣＲ）１２は、イメージデータをファクシミリ通信の規約に従って圧縮コードに変換する。

なお、この本体４内には、図示しないがマウス５用のマウスインタフエース，スキャナ用のスキャナインタフエース等を備えている。

第４図はシステム制御部９の一例を示すブロック図である。

このシステム制御部９は、このシステム全体の制御を司る１６ビットマイクロプロセッサ等からなるＣＰＵ２１と、このＣＰＵ２１とコモンバスとの間に介在したバスバッファ２２と、タイミングジェネレータ２３と、リフレッシュコントローラ２４とを有する。

また、このシステム制御部９は、ＯＳや文書受信にかかわるプログラム等の常駐プログラムが常駐するシステム領域及びその他の領域からなる例えば５１２ＫＢの容量を有するＲＡＭ２５と、このＲＡＭ２５を制御するＲＡＭコントローラ２６，２７と、電源投入時にＨＤＤ７からＲＡＭ２５へのプログラムロードを制御するブートプログラムを格納したブートＲＯＭ２８とを備えている。

さらに、このシステム制御部９は、キーボード１との間の情報転送を司るキーボードインタフエース（Ｉ／Ｆ）３０と、ＨＤＤ７を制御するハードディスクインタフエース（ＨＤＤＩ／Ｆ）３１と、このＨＤＤＩ／Ｆ３１とコモンバスとの間に

介在したバッファ３２と、ＦＤＤ８を制御するフロッピディスクコントローラ（ＦＤＣ）３３とをも備えている。

さらにまた、このシステム制御部９は、シリアルポート（ＳＩＯ）３４，３５をも備えている。

第５図はＣＲＴＣＵ１０の一例を示すブロック図である。

このＣＲＴＣＵ１０は、全体の制御を司る１６ビットマイクロプロセッサ等からなるスレーブＣＰＵ４１と、スレーブＣＰＵバスとコモンバスとの間に介在したバスＩ／Ｆ４２と、ＩＰＬ用の例えば１６ＫＢ容量のＲＯＭ４３と、システム制御部９と共有する共有メモリ及びプログラムメモリ用のＲＡＭ４４とを備えている。

このＲＡＭ４４で構成する共有メモリは、インデックスバッファと、管理領域と、レコード領域と、ＦＡＸ送信用データバッファと、プリンタ用ページバッファと、イメージ編集用データバッファとからなる。

また、このＣＲＴＣＵ１０は、スレーブＣＰＵバスとマイクロバスとの間に介在したバスＩ／Ｆ４５と、マイクロプログラム用のＲＯＭ４６と、プログラムコントロールメモリ用のＲＡＭ４７とを備えている。

さらに、このＣＲＴＣＵ１０は、漢字パターン用ＲＯＭ，レイアウトデータ用ＲＯＭ，システム用ＲＯＭ，外字パターン用ＲＡＭからなるキャラクタ・グラフイック（ＣＧ）メモリ４８と、ＣＲＴコントローラ４９とを備えている。

さらにまた、このＣＲＴＣＵ１０は、ディスプレイ装置（ＣＲＴ）２の表示データを展開する画像メモリ５１と、表示タイミングを制御するタイミング発生回路５２と、プリンタ３との間のデータ転送を司るプリンタＩ／Ｆ５３とを備えている。

第６図は通信制御部（ＣＣＵ）１１の一例を示すブロック図である。

この通信制御部１１は、全体の制御を司る１６ビットマイクロプロセッサ等からなるＣＰＵ６１と、コモンバスとの間に介在したパラレルインタフエース６２と、テレテックス通信制御及びファックス通信制御プログラムを格納したＲＯＭ６３と、主としてワーキングメモリ用のＲＡＭ６４と、メモリ間通信を行なうために受信文書情報及び送信文書情報並びに送受信ログ情報を格納する通信メモリとして使用するＲＡＭ６５とを備えている。

また、この通信制御部１１は、公衆電話回線を介して相手側端末装置との間で通信を行なうために、マルチプロトコル・シリアルコントロール（ＭＰＳＣ）６６，モデム（ＭＯＤＥＭ）６７，ラインインタフエース６８，回線制御装置（ＡＡ－ＮＣＵ）６９，ターミナル７０，回線保護装置（ＰＤ）７１並びにモデム６７，回線制御装置６９用のモデムインタフエース７２，ＮＣＵインタフエース７３とを備えている。

さらに、この通信制御部１１は、送受信日時の管理等に使用するカレンダ７４と、内部の状態設定用スイッチ（ＬＰ／ＳＷ）７５と、受信文書有り等を表示するための表示器インタフエース７６及びＬＥＤ表示器７７をも備えている。

なお、この通信制御部１１は、図示を省略するが、公衆電話回線だけでなく、パケット交換網あるいは回線交換網をも使用可能にするためのＸ．２１インタフエース及びコネクタをも有している。

第７図はＤＣＲ１２の一例を示すブロック図である。

このＤＣＲ１２は、ＣＰＵ８１，ＲＯＭ８２及びローカルＲＡＭ８３からなるマイクロコンピュータ・システムによつて全体を制御する。

共有メモリ８４は、このＤＣＲ１２とシステム制御部９（ホスト）とで共有するメモリであり、コマンド・レスポンスを格納するコマンド・レスポンスエリアと、圧縮するイメージデータ（画情報データ）を格納するイメージデータエリアと、圧縮したイメージデータ(画情報)を格納する圧縮コードエリアとからなる。

ＦＣＰ（ファクシミリ・コントロール・プロセッサ）８５は、共有メモリ８４のイメージデータエリアに書込まれたイメージデータを圧縮して、圧縮後の圧縮コード（画情報）を共有メモリ８４の圧縮コードエリアに書込む。

反転データゲート８６は、共有メモリ８４に対する書込みデータ又は共有メモリ８４からの読出しデータのビット並びを反転（逆転）して通過させ、非反転データゲート８７は、共有メモリ８４に対する書込みデータ又は共有メモリ８４からの読出しデータのビット並びをそのままにして通過させる。

アドレスデコーダ８８は、コモンバスからのアドレスデータをデコードして、反転データゲート８６を選択するゲートリクエストＡＲＥＱ，非反転データゲート８７を選択するゲートリクエストＢＲＥＱ，共有メモリ８４に対するホスト側の使用を要求するホストリクエストＨＯＳＴ及びレジスタセレクトＲＥＧＳＬ，カードセレクトＣＳＬ等を出力する。

セレクタ８９は、ＦＣＰ８５からの共有メモリ８４の使用を要求するＤＣＲリクエストＤＣＲＲＱ及びアドレスデコーダ８８からのホストリクエストＨＯＳＴに応じて、共有メモリ８４に対するデータ入出力ラインをＦＣＰ８５又は反転データゲート８６，非反転データゲート８７に選択的に切換えると共に、共有メモリ８４に対するアウトイネーブルＯＥ，ライトイネーブルＷＥを出力し、またバスフラグＢＵＳＦＡＬＧを出力する。

アドレスデコーダ９０は、ＣＰＵ８１からのアドレスデータに応じてＦＣＰ８５に対して共有メモリセレクトＣ－ＲＡＭＳＬ，ＦＣＰセレクトＦＣＰＳＬを出力し、ＲＯＭ８２に対してＲＯＭセレクトＲＯＭＳＬを、ローカルＲＡＭ８１に対してローカルＲＡＭセレクトＲＲＡＭＳＬを、夫々出力する。

なお、このＤＣＲ１２は、この他コマンドステータスレジスタ９１及び割込みフラグ９２等をも備えている。

第１図はこの端末装置の機密保護制御に係わる部分を機能的に示すブロック図である。

入力部１０１は文字情報，文書作成編集に必要な制御情報，文書送信に必要な制御情報を入力し、機密指示部１０２は文書の機密とする文字を指示する入力をし、機密レベル指示部１０３は機密指示をした文字の機密レベルの指示を入力する。なお、これ等はキーボード１の各キーに相当する。

入力判別部１０４は、これ等の入力部１０１，機密指示部１０２及び機密レベル指示部１０３からの入力される情報が文字情報，文書作成制御情報，機密指示情報及び機密レベル指示情報か送信制御情報あるいはパスワード情報等のいずれであるかを判別して、この判別結果に応じて入力された情報を各部に送出する。この入力判別部１０４はシステム制御部７の入力制御部に相当する。

表示部１０５は文書情報等を表示し、印刷部１０６は文書情報等を印刷し、出力制御部１０７はこれ等の表示部１０５及び印刷部１０６の制御を司る。これ等はそれぞれＣＲＴディスプレイ装置２，プリンタ３及びＣＲＴＣＵ１０に相当する。

外部記憶部１０８は文書情報，コシステムプログラム等を格納し、外部記憶制御部１０９は外部記憶部１０８に対する情報の書込み及び読出しを制御する。これ等はそれぞれハードデイスクドライブ装置７，フロッピデイスクドライブ装置８及びシステム制御部９の内のＨＤＤＩ／Ｆ３１及びＦＤＣ３３に相当する。

通信制御部１１０は相手先端末装置との間におけるテレテツクス通信及びフアクシミリ通信制御をし、通信制御部１１に相当する。

文書作成編集制御部１１１は、入力判別部１０４を介して入力される文字情報，文書作成制御情報，機密指示情報及び機密レベル指示情報を受けて文書の作成編集をし、出力制御部１０７を介して編集文書を表示部１０５に表示させたり印刷部１０６で印刷させ、また文書を外部記憶制御部１０９を介して外部記憶部１０８に格納したり読出したりする。

また、この文書作成編集制御部１１１は、機密指示情報が入力されたときには当該文書の指定された文字情報に機密開始情報及び機密終了情報を付加して、また機密レベル指示情報が入力されたときには機密情報に機密レベル情報を付加する。

さらに、この文書作成編集制御部１１１は外部記憶部１０８に格納された文書の読出しが指示さ

れたときに当該文書にパスワード（特定の文字列）が付加されているときにはパスワード制御部１１２に対して登録パスワードと入力されるパスワードとの比較制御をさせる。

さらにまた、この文書作成編集制御部１１１は、外部記憶部１０８に格納されている受信文書の読出しが指示されたときには、読出した文書の文字情報を出力可能かを機密情報検出部１１３，機密レベル検出部１１４，レベル判定部１１５によつて判定させ、この判定結果に応じて文字情報の出力制御をする。

パスワード制御部１１２は、文書作成編集制御部１１１からの比較制御指示を受けたときに、外部記憶制御部１０９を制御して文書パスワードファイルを読出して指定された文書の登録パスワードを抽出し、出力制御部１０７を介して表示部１０５にパスワード入力指示を表示させて入力部１０１から入力判別部１０４を介して入力されたパスワードと登録パスワードとを比較してこの比較結果を文書作成編集制御部１１１に通知する。

機密情報検出部１１３は文書作成編集制御部１１１から送られてくる情報が機密情報か否かを検出し、機密情報であるときには機密レベル検出部１１４にその旨を通知する。機密レベル検出部１１４は機密情報検出部１１３から機密情報検出通知を受けたときにその機密レベル情報を検出して、レベル判定部１１５に送出する。レベル判定部１１５は機密レベル検出部１１４から送られてきた機密レベル情報と装置レベル記憶部１１６に予め記憶されている装置の機密レベルとを比較して、この比較結果を文書作成編集制御部１１１に通知する。

ローカル送受信制御部１１７は入力部１０１から入力判別部１０４を介して送信指示を受けたときに外部記憶部１０９を制御して外部記憶部１０８から指定の送信文書を読出して通信制御部１１０に送出し、また通信制御部１１０から送られてくる受信文書を外部記憶部１０９を制御して外部記憶部１０８に格納する。

次に、このように構成したこの実施例の作用について第８図以降をも参照して説明する。

まず、この文書作成通信端末装置における文書送信処理について第８図を参照して説明する。

図示しない作業選択処理においてテレテツクス通信メニューの内の文書送信が選択されたときには、まず画面上に文書送信の送信条件設定のメニューを表示し、キー操作で設定される送信モード（通常送信，緊急通信等），送信時刻，文書内容（日本文等）を取込む送信条件設定処理をする。

この送信条件設定処理終了後、文書ファイルに登録された文書名を読出して、文書名一覧表のメニューを画面上に表示し、キー操作で指定される送信する文書名を取込む文書指定処理をする。

この文書指定処理終了後、宛先ファイルから登録されている宛先リストを読出して宛先指定のメニューを表示し、キー操作で指定される宛先名を取込む宛先指定処理をする。

この宛先指定処理終了後、宛先名，文書名等の確認用表示をして、キヤンセルであればキヤンセル処理に移行し、確認されれば以下に述べる送信準備処理に移行する。

この送信準備処理では、システム制御部（ＳＣＵ）９は、まず指定された宛先名のアドレス（ダイアル・ナンバ），送信文書名及び送信時刻等の送信情報を通信制御部１１に渡す。

一方、通信制御部（ＣＣＵ）１１は、ＳＣＵ９からの所定のコマンドによつて第９図に示す処理の実行を開始して、ＳＣＵ９から送られてくる送信情報を受領する。

なお、ＣＣＵ１１が相手側と文書通信を行なつているとき等ＳＣＵ９からの情報を受付けられないときには、その通信が終了するまでＳＣＵ９との間での送信情報の送受等この処理を待機する。

その後、ＳＣＵ９は、宛手先の宛先リストに登録されているモードあるいはキー入力されたモードを読込んでフアツクス（ＦＡＸ）モードかテレテツクス（ＴＥＬＥＴＥＸ）モードかを判別する。

そして、送信モードがＦＡＸモードであれば、ＣＣＵ１１に対してファイルＮｏ．を要求し、ＣＣＵ１１はこのファイルＮｏ．要求に対して所定

のファイルＮｏ．を送出する。なお、このファイルＮｏ．は内部処理用のファイルＮｏ．であり、例えばテレテックスモードでは「ＴＤＯＣ－ＸＸＸ」を使用する。

そこで、ＳＣＵ９は、このＣＣＵ１１から受領したファイルＮｏ．をテレテックスモードの「ＴＤＯＣ－ＸＸＸ」からＦＡＸモードの「ＦＤＯＣ－ＸＸＸ」に変更する。

そして、ＳＣＵ９は、ＦＤＤ８から指定された送信文書を読出して、その文書を変更後のファイルＮｏ．「ＦＤＯＣ－ＸＸＸ」を付してＨＤＤ７で構成した送信ファイルに登録すると共に、変更後のファイルＮｏ．をＣＣＵ１１に返送する。

これに対して、送信モードがＦＡＸモードでなければ、すなわちＴＥＬＥＴＥＸモードであれば、同様にＣＣＵ１１に対してファイルＮｏ．を要求する。

そして、ＣＣＵ１１から受領したテレテックス用のファイルＮｏ．「ＴＤＯＣ－ＸＸＸ」をそのまま指定された送信文書に付してその送信文書を送信ファイルに登録する。

なお、ＣＣＵ１１は、ＳＣＵ９からファイルＮｏ．の返送を受けたときには、ＳＣＵ９に対して送出したファイルＮｏ．をＳＣＵ９から受領したファイルＮｏ．に変更して再登録する。

次に、システム制御部９及び通信制御部１１が実行する送信処理について第１０図及び第１１図を参照して説明する。

通信制御部（ＣＣＵ）１１は、送信時刻が指示されているときにはその時刻になつた時に、また送信時刻が指示されないときには直ちに送信開始と判断して、送信ステータスをＯＮにする（送信要求をする）。

一方、システム制御部（ＳＣＵ）９は、ＣＣＵ１１を所定の時間間隔でポーリングして送信ステータスがＯＮになつたか否かをチエツクして、送信ステータスがＯＮになつたとき、すなわち送信要求があつたときには、ＣＣＵ１１に対して送信するファイルＮｏ．（送信ファイルＮｏ．）を要求する。

一方、ＣＣＵ１１は、送信ファイルＮｏ．要求を受けたときにはＳＣＵ９に対して送信ファイルＮｏ．を送出してＳＣＵ９からのコマンドを待つ。

そこで、ＳＣＵ９は、ＣＣＵ１１から受領した送信ファイルＮｏ．が「ＴＤＯＣ－ＸＸＸ」か「ＦＤＯＣ－ＸＸＸ」かをチエツクして、ＦＡＸモードで送信する文書かを判別する。

このとき、その送信ファイルＮｏ．がＦＡＸモードのファイルＮｏ．であれば、ＣＣＵ１１に対してＦＡＸ送信ドキュメント・コマンドを送出し、ＴＥＬＥＴＥＸモードのファイルＮｏ．であればＴＥＬＥＴＥＸ送信ドキュメント・コマンドを送出する。

そこで、ＣＣＵ１１は、ＳＣＵ９から受領したコマンドがＦＡＸ送信ドキュメント・コマンドか否かを判別して、この判別結果に応じてファクシミリ通信又はテレテックス通信の規約に従つて送信先（相手先）との間の回線接続処理をする。

そして、相手先との回線が接続される等して送信可になつたときには、ＳＣＵ９及びＣＣＵ１１との間で送信モード（ＦＡＸ／ＴＥＬＥＴＥＸ）に従つて送信文書をＳＣＵ９からＣＣＵ１１に渡す送信文書送出及び送信文書受領処理をする。

その後、ＣＣＵ１１は、ＳＣＵ９から受領した送信文書情報を送信モード（ＦＡＸ／ＴＥＬＥＴＥＸ）に応じて相手先に送信する。

そして、ＳＣＵ９は、ＣＣＵ１１への送信文書の送出終了後、また送信不可のときには直ちに送信終了処理をし、ＣＣＵ１１は、相手先への文書送信終了後、また回線接続が不可のときには直ちに送信終了処理をして、一連の処理を終了する。

次に、文書作成処理の一例について第１２図を参照して説明する。

この文書作成処理では、キーボード１からのキー入力を待ち、キーボード１からのキー入力が有ると、そのキー入力が文字キーか否かを判別する。

このとき、キー入力が文字キーであれば入力された文字コードを文書編集エリアの書込みポインタで示されるアドレスに格納すると共に、入力された文字をＣＲＴディスプレイ装置２に表示した

後、キー入力待機に戻る。

また、キー入力が文字キーでなければ、キーボード1に付設した単独キー又は複数キーの組合せからなる機密設定キーによる機密設定指示か否かを判別する。

そして、機能設定指示であれば、予め定めた機密開始情報としての機密モードオンコードを文書編集エリアの書込みポインタで示されるアドレスに格納する。

その後、CRTディスプレイ装置2に機密レベル設定入力促進文字を表示して機密設定をする文字の機密レベル（これを「文書機密レベル」と称する）の設定要求をし、キーボード1から入力される機密レベル情報としての機密レベルコードを文書編集エリアの書込みポインタで示されるアドレスに格納する。

なお、この機密レベルの設定は、例えば新規機密レベルの設定，前回設定した機密レベルの設定及び予め設定した装置の機密レベルを機密レベルとする設定のいずれかの選択を促すメニューを表示して、その選択結果に応じてキーボード1から入力される機密レベルコード，前回格納した機密レベルコードあるいは装置の機密レベルコードを格納するようにしている。

また、この文書機密レベルは例えば「0～255」の256段階を設定することができ、機密レベル「0」を最上位の機密レベルとしている。更に装置の機密レベルも同様に「0～255」の256段階を設定することができ、機密レベル「0」を最上位の機密レベルとしている。この装置の機密レベルはシステムジエネレーション時に設定するようにしているが、機密レベル設定スイッチを設けてこのスイッチで設定するようにすることもできる。

その後、キー入力を待ち、キー入力があればそのキー入力がキーボード1に付設した単独キーズは複数キーの組合わせからなる機密解除キーによる機密解除指示か否かを判別する。

このとき、キー入力が機密解除指示でなければ、キー入力が文字キーか否かを判別して、文字キーであればその入力文字コードを文書編集エリアの書込みポインタで示されるアドレスに格納して表示した後、また文字キーでなければそのキー入力に応じたその他の処理をした後、キー入力待機に戻る。

そして、機密解除キーによる機密解除指示がキー入力されたときには、機密終了情報としての予め定めた機密モードオフコードを文書編集エリアの書込みポインタで示されるアドレスに格納した後、キー入力待機に移行する。

さらに、キー入力が機密設定キーによる機密設定指示でなければ、編集終了キーか否かを判別して、編集終了キーであれば、現作成中の文書の登録文書名を取込む処理をした後、当該文書のパスワードを取込む処理をする。なお、文書にパスワードを付加するか否かは任意に選択することができる。そして、当該作成文書をフロッピディスクドライブ装置8に登録する。

次に、文書作成処理の他の例について第13図を参照して説明する。

この文書作成処理では、キーボード1からのキー入力があり、このキー入力がキーボード1に付設した単独又は複数のキーの組合わせからなる機密モードキーによる入力であれば、文書編集エリアの書込みポインタで示されるアドレスに機密モードオンコードを挿入する。

その後、前述した文書作成処理と同様にして機密レベルの設定処理をした後、キーボード1からのカーソル移動指示入力を受けて指定された位置にカーソルを移動する処理をし、キーボード1に付設した実行キーが押されるまでこのカーソル移動処理を繰返し実行する。

そして、実行キーが入力されたときに、文書編集エリアの書込みポインタで示されるアドレスに機密モードオフコードを挿入した後、機密モードオンコードと機密モードオフコードとの間の文字を予め定めた代用文字（空白，網かけ，その他の予め定めた文字等）に置き換えて表示する。

なお、その他の処理については前述した文書作成処理と同様である。

これ等の文書作成処理について第１４図及び第１５図をも参照して具体的に説明する。

ここでは、第１４図（イ）に示す文書を新規に作成し、この文書の「原価：１００万」の内の「１００」について機密保護を行なうものとする。

この場合、まず第１２図に示した文書作成処理による場合には、「原価：」まで入力した後、機密設定キーを押し下げて機密設定指示をすることによつて、第１５図に示すように文書編集エリアには「原価：」の次のアドレスに機密モードオンコード（「モードＯＮ」で示す）が格納され、この機密設定の機密レベル（文書機密レベル）を設定することによつて「モードＯＮ」の次のアドレスに文書機密レベルコード（「文書レベル」で示す）が格納される。

その後、「１００」をキー入力することにより、「文書レベル」の次アドレスから「１００」が順次格納され、そこで機密解除キーを押し下げて機密解除を指示することによつて「１００」の次のアドレスに機密モードオフコード（「モードＯＦＦ」で示す）が格納され、更に「万」をキー入力することによつて「モードＯＦＦ」の次のアドレスに「万」が格納される。

このようにして秘密にしたい「１００」が機密モードオンコードと機密モードオフコードとで囲まれ、この文字列が機密範囲として設定される。すなわち、この文書作成処理においては、文書を作成するための文字入力の途中で機密範囲の設定をするようにしている。

次に、第１２図に示す文書作成処理による場合には、「原価：１００万」まで入力した後、カーソルを「１００」の「１」に位置させて機密モードキーを押し下げることによつて、上述した場合と同様に「１」の前に機密モードオンコードが挿入格納され、そして機密レベルを指示することによつて文書機密レベルコードが次アドレスに挿入格納される。

その後、カーソルを２つ目の「０」に位置させて実行キーを押すことによつて、その「０」の後に機密モードオフコードが挿入され、表示されている「１００」が例えば第１４図（ロ）に示すような代用文字（網かけ）表示に置換わる。すなわち、この文書作成処理では、機密範囲の設定を上述した文書作成処理とは異なり一旦文書を作成した後行なうようにしている。それと共に、機密設定をした文字について文書作成段階で代用文字に置換えて表示しているので、機密文書の作成編集中に作成者以外の者に編集文書を見られても機密を知られない。

なお、上述した２種類の文書作成処理を組合せることもできる。すなわち、文字入力時に機密範囲を設定し、機密設定された文字については代用文字で表示するようにしたり、また文字入力後機密範囲を設定し、機密設定された文字は作成中は代用文字に変更しないようにすることもできる。

次に、登録文書出力処理について第１６図を参照して説明する。なお、この登録文書出力処理は例えば文書更新時や文書印刷時等に実行する。

この登録文書出力処理では、まず読出す登録文書名を取込んでこの登録文書名の文書があるか否かを判別し、文書があればその文書が受信文書か否かを判別する。この文書が受信文書か否かの判別は例えば受信文書ファイルに格納している受信文書名ファイルと登録文書名とを比較して行なうことができる。

そして、読出し文書が受信文書でないときには、当該文書にパスワードが付加されているか否かを、例えば各文書についてのパスワードを格納した文書パスワードファイルをチエツクして判別する。

このとき、パスワードが付加されていれば、ＣＲＴディスプレイ装置２にパスワード入力要求を表示して、入力されるパスワードと当該文書に登録されているパスワードとが一致したか否かを判別する。

そして、入力されたパスワードと登録されているパスワードとが一致したとき、または文書にパスワードが付加されていないときには、指定された文書を文書ファイルから読出して、その文書を出力（表示ないし印刷）する文書出力処理をする。

すなわち、文書作成時に機密保護が設定された

文書であつてもパスワードが付加されていないとき、及びパスワードが付加されていてもそのパスワードが入力されたときには、機密を解除して文書のすべての内容を出力する。それによつて、機密保護を設定した文書であつても作成者はすべての内容を出力することができる。

これに対して、読出し文書が受信文書であるとき、及び受信文書でないがパスワードが付加されてそのパスワードが入力されないときには、指定された文書を一旦内部メモリに読込む。

そして、その読込んだ文書からデータを読出し、まずそのデータが機密モードオンコードか否かを判別し、機密モードオンコードであれば次のデータすなわち機密レベルコードを読出して、文書機密レベルが装置の機密レベルより高い（文書＞装置）か否かを判別し、文書機密レベルが装置の機密レベルより高いときには機密モードフラグFをF＝1にセットする。

また、読出しデータが機密モードオンコードでなければ、そのデータが機密モードオフコードか否かを判別して、機密モードオフコードであれば機密モードフラグFを「0」にリセットする。

さらに、読出しデータが機密モードオフコードでなければ、そのデータが文字データか否かを判別して、文字データがあれば機密モードフラグFがF＝1か否か、すなわち機密モードが指定された文字でその機密レベルが装置の機密レベルより高いかを判別し、機密モードフラグF＝1であればその文字は出力できないので予め定めた代用文字を出力し、機密モードフラグF＝0であればその読出した文字を出力する。

さらにまた、読出しデータが文字データでもなければ、その読出しデータに応じた処理をする。

そして、これ等の各処理のいずれかを実行した後、文書終了か否かを判別して、文書終了になるまで同様の処理を繰返し実行する。

したがつて、例えば前述したように機密設定された第14図に示すような受信文書を受領したときには、この文書の「原価：」まではすべての文字が出力され、次のデータを読出すとこのデータは「機密モードオンコード（モードON）」であるので次のデータすなわち「文書機密レベルコード」を読出し、このとき文書機密レベルが装置の機密レベルよりも高いとすると機密モードフラグF＝1にセットされる。

それによつて、「文書機密レベルコード」の次のデータを読出すとこのデータは文字データ「1」であり、しかもこのとき機密モードフラグF＝1であるので、この文字「1」は表示されないで代用文字（例えば網かけ）が表示される。更に次の文字「0」，「0」についても同様に代用文字が表示される。

そして、次のデータを読出すとこのデータは「機密モードオフコード（モードOFF）」であるので機密モードフラグF＝0にリセットし、次のデータを読出したときにはこの読出しデータだある文字「万」が表示される。

このようにして、受信文書については機密モードオンコードと機密モードオフコードで囲まれた設定機密範囲の文字については文書機密レベルが装置機密レベルよりも高いときには表示されないので、機密を保護ができる。また、受信文書でない場合でも設定機密範囲の文字は編集対象とならないので作成者以外によつて変更されることがなく機密を保護できる。

このように、この文書作成通信端末装置においては、文字単位で機密を設定できるので、文書の利用性が向上し、また文書送信時に文書の一部を機密にして送信することができ、相手先での受信文書の利用性が向上する。

また、従来の文書作成通信端末装置においては、文書全体でなく文書の一部を機密にしたいような文書を送信する場合には、受信側の機密レベルに応じて秘密としたい部分を空白あるいは網かけ等のマスキング処理をした後文書を送信しなければならず、このような機密文書の送信に手間がかかつた。しかも、複数の端末装置に対して同一文書を送信する場合でも、受信側のレベルに応じたマスキング処理を施した文書が必要になり、同報装置を使用することが困難であつた。

これに対して、この文書作成[redacted]端末装置のように文書の文字単位で機密設定ができるようにし、かつその機密レベルを示す情報を付加することによつて、機密レベルの異なる複数の相手先に送信する場合でも文書は1つで済み同報装置を使用できるので文書送信が容易になる。

なお、上記実施例においては、この発明を文書作成通信端末装置に実施した例について述べたが、例えば通信機能を持たない文書作成編集装置やデータ処理装置等その他の情報処理装置にも実施することができる。

また、上記実施例においては機密文書を送信するときに当該文書にパスワードを付加しないで送信する例について述べたが、パスワードを付加して送信する機能を持たせ、受信側でパスワードを入力することによつて機密を解除できるようにするようにしてもよい。このパスワードの送信は、例えばテレテツクスにおいてはＣＣＩＴＴ勧告Ｓ．６２のエンドツーエンド制御手順におけるセツシヨン又はドキユメント制御手順で規定される私用パラメータを使用[redacted]行なうことができる。

効　果

以上説明したように、この発明によれば、文書の一部に機密保護を設定でき、文書の利用性が向上する。

4.図面の簡単な説明

第１図はこの発明の一実施例を示すブロツク図、

第２図はこの発明を実施した文書作成通信端末装置の一例を示す外観斜視図、

第３図は同じくその本体の内部構成の一例を示すブロツク図、

第４図は同じくシステム制御部を示すブロツク図、

第５図は同じくＣＲＴＣＵを示すブロツク図、

第６図は同じく通信制御部のブロツク図、

第７図は同じくＤＣＲのブロツク図、

第８図及び第９図はシステム制御部及び通信制御部が実行する文書送信処理及び文書送信準備処理の一例を示すフロー図、

第１０図及び第１１図は同じく送信処理の一例を示すフロー図、

第１２図及び第１３図は同じく文書作成処理の異なる例を示すフロー図、

第１４図及び第１５図は同じくその文書作成処理の具体的説明に供するフロー図、

第１６図は同じく登録文書出力処理の一例を示すフロー図である。

１０１…入力部　　１０２…機密指示部

１０３…機密レベル指示部

１０５…表示部　　１０６…表示部

１０８…外部記憶部　　１１０…通信制御部

１１１…文書作成編集制御部

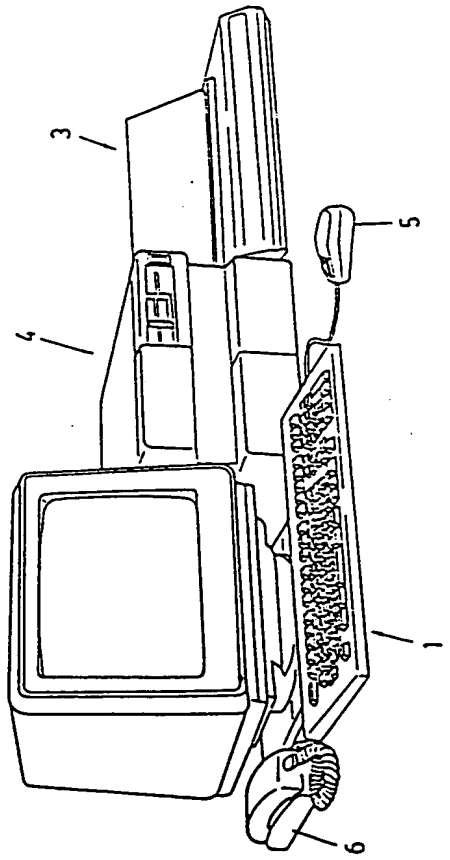
１１３…機密情報検出部

１１４…機密レベル検出部

１１５…機密レベル判定部

１１６…装置レベル記憶部

第２図



出願人　株式会社　リ　コ　ー

代理人　弁理士　大　澤　敬

同　同　稲　元　富　保

Fig. 1
第1図

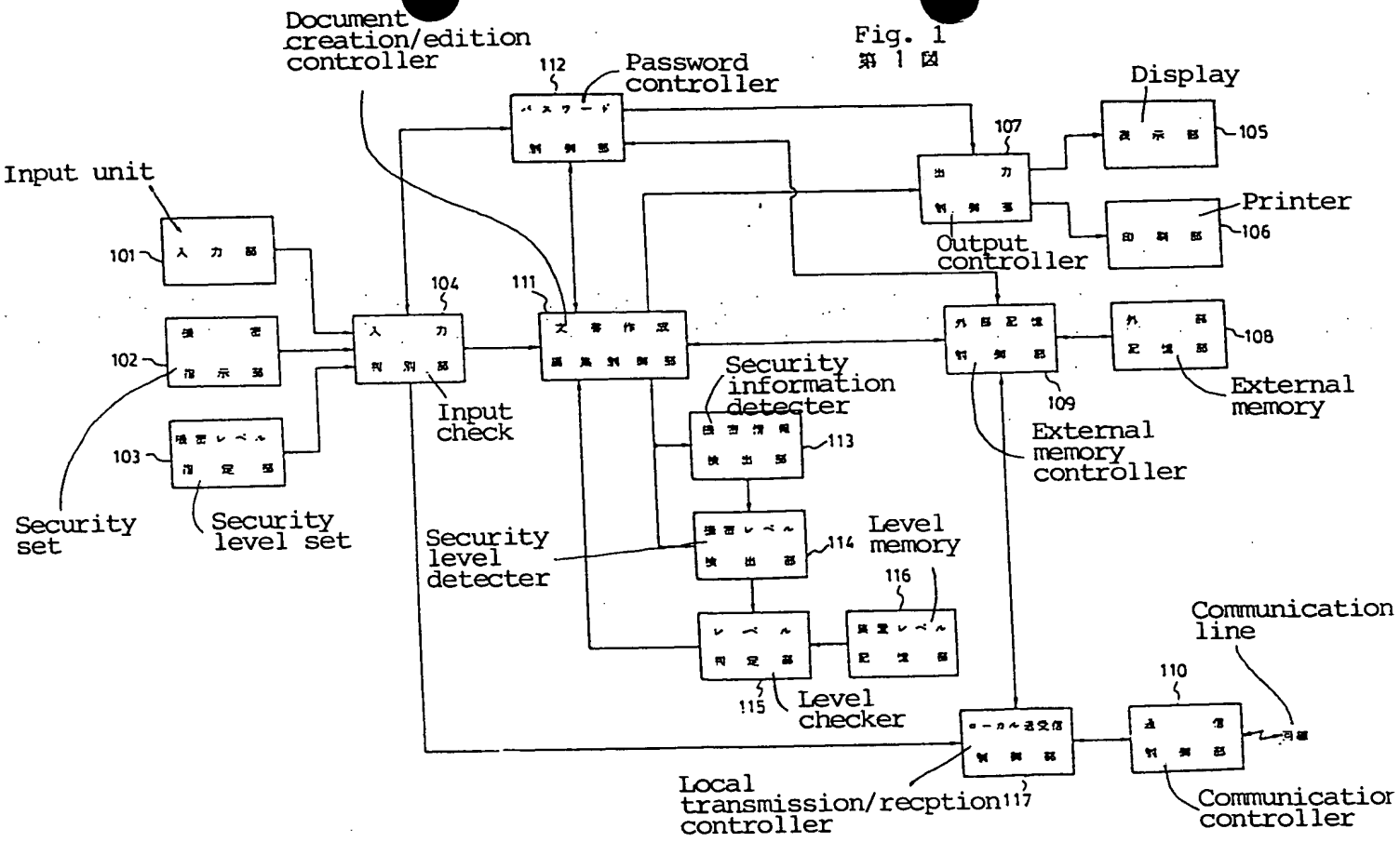


Fig. 3
第3図

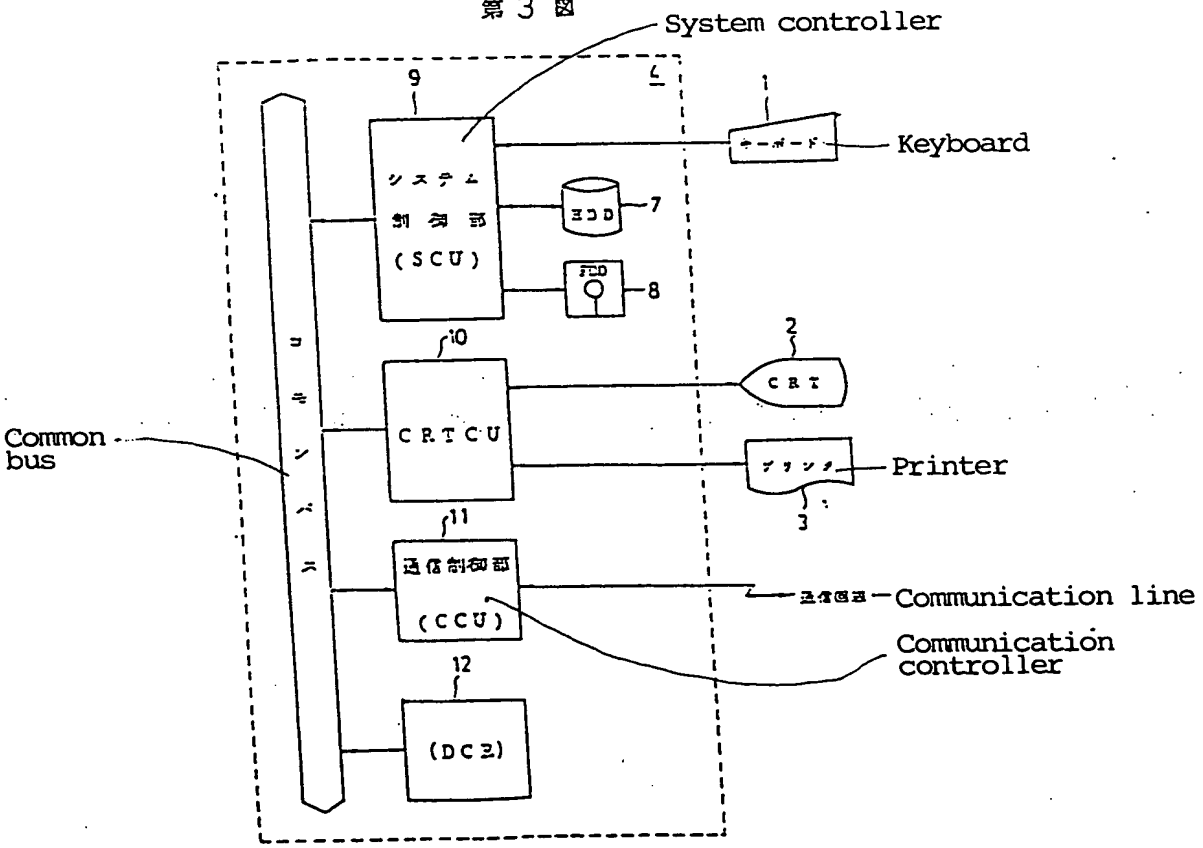


Fig. 4
第4図

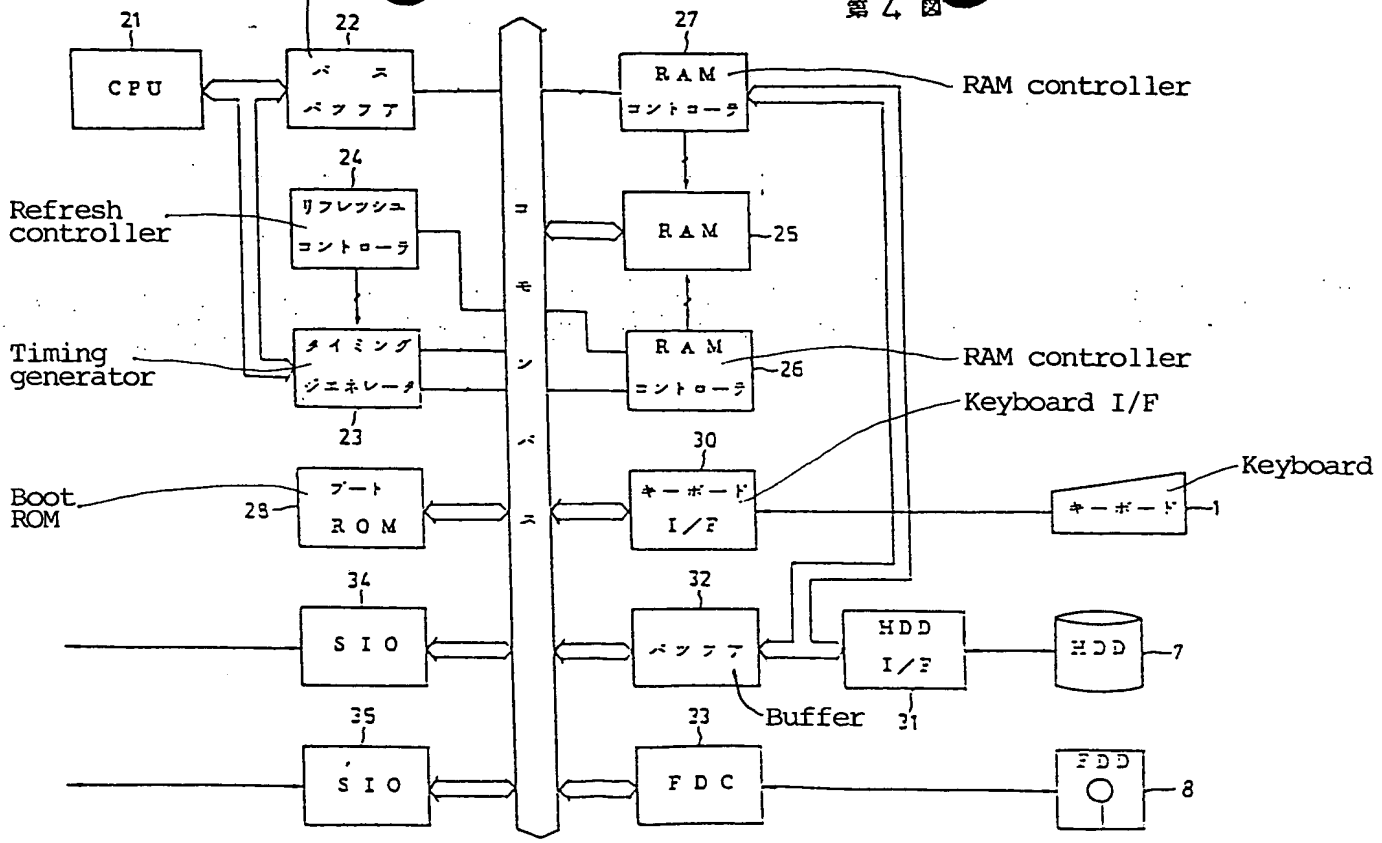


Fig. 5
第5図

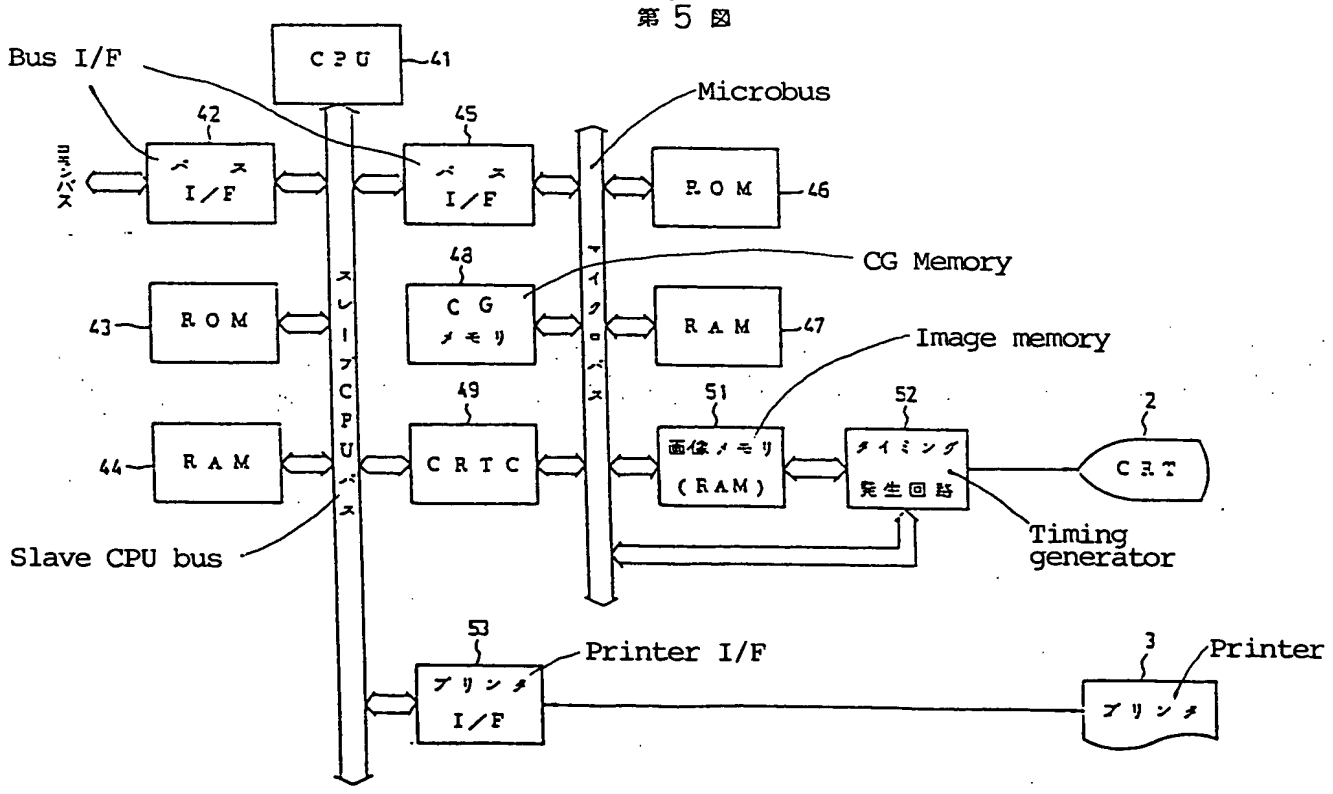


Fig. 7
第7図

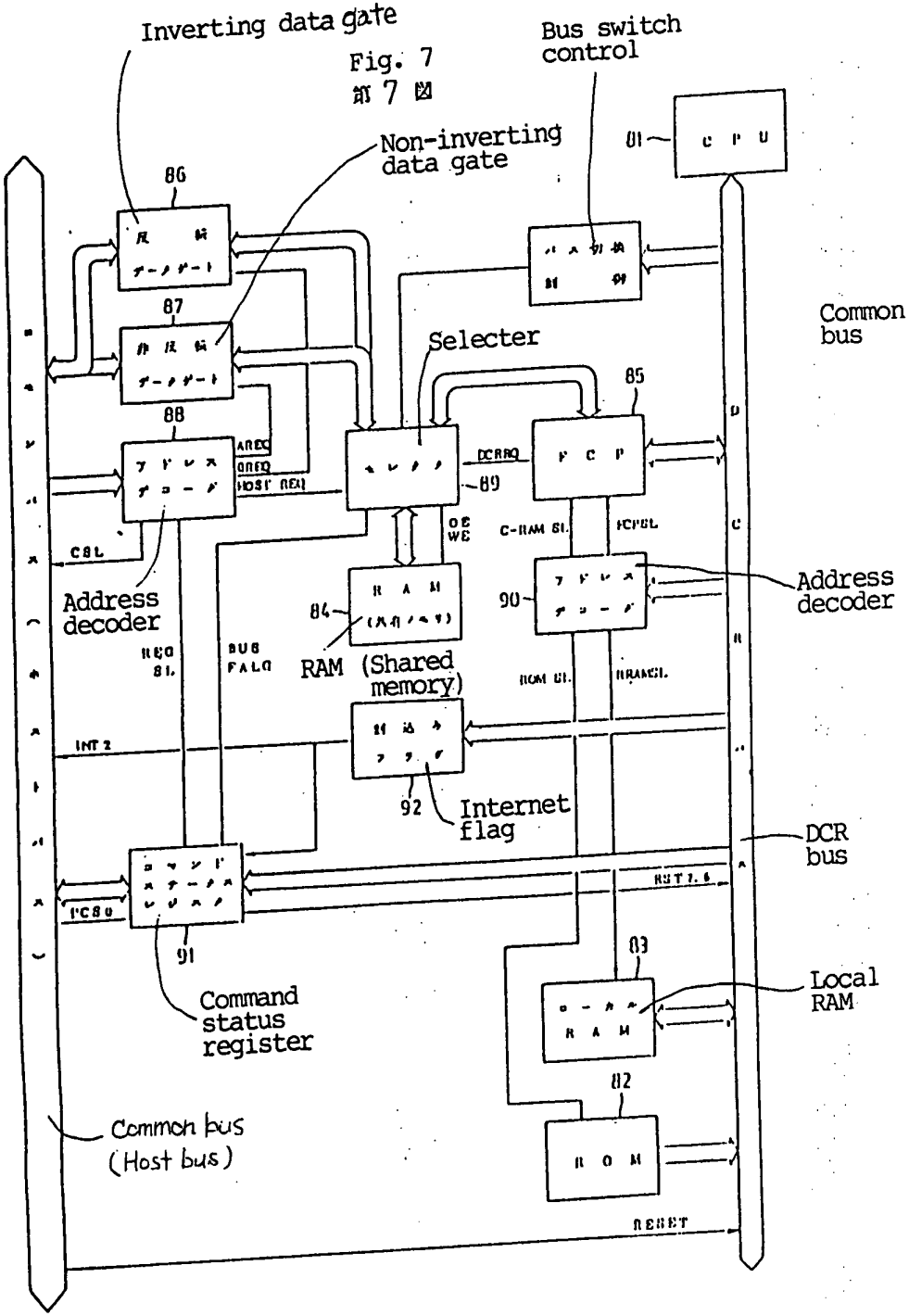
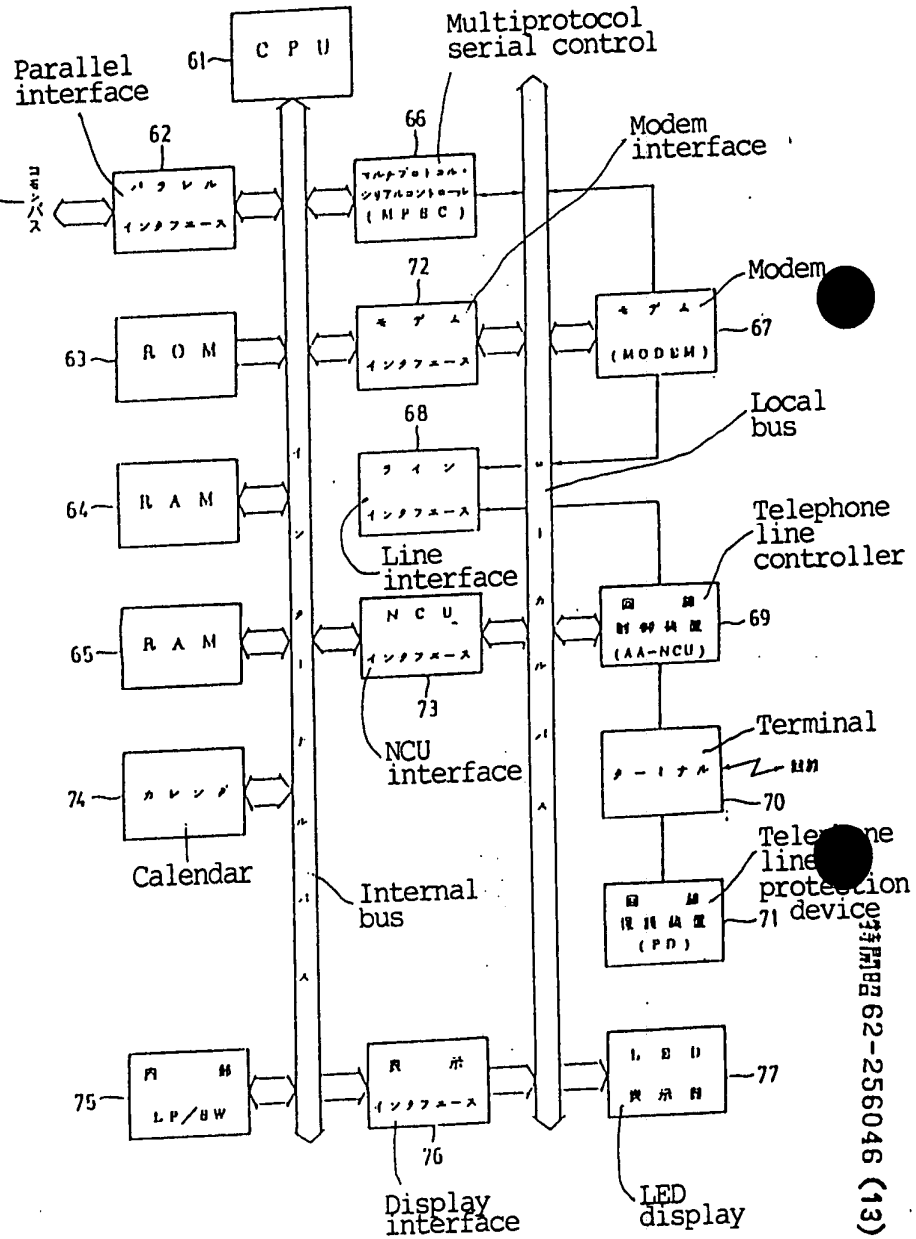


Fig. 6
第6図



特開昭62-256046 (13)

Fig. 10
第10図

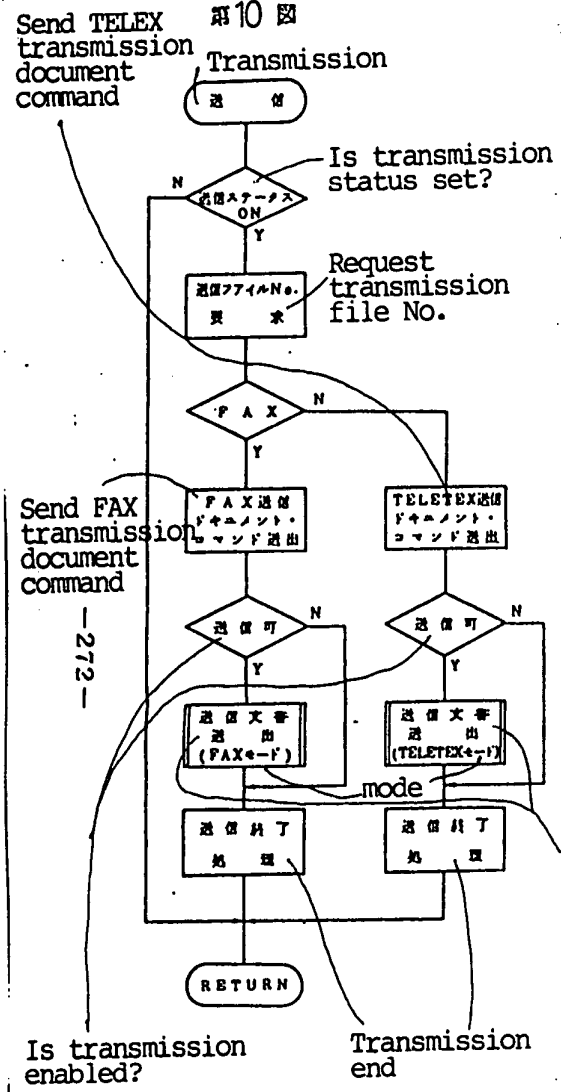


Fig. 11
第11図

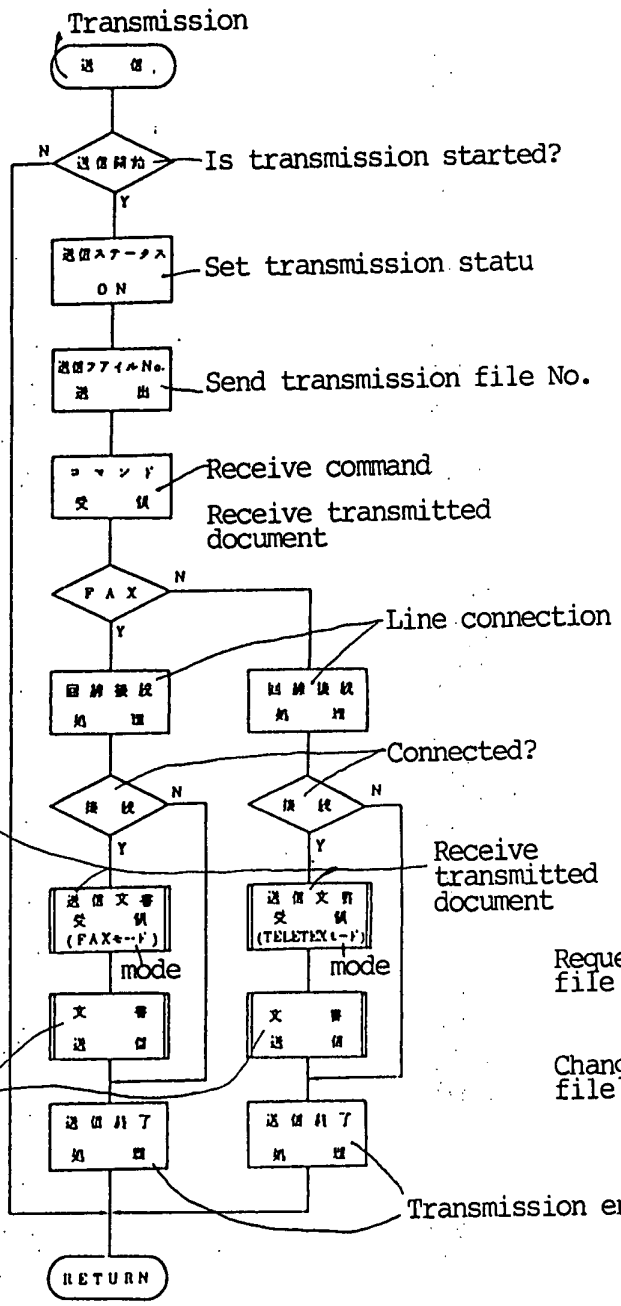


Fig. 8
第8図

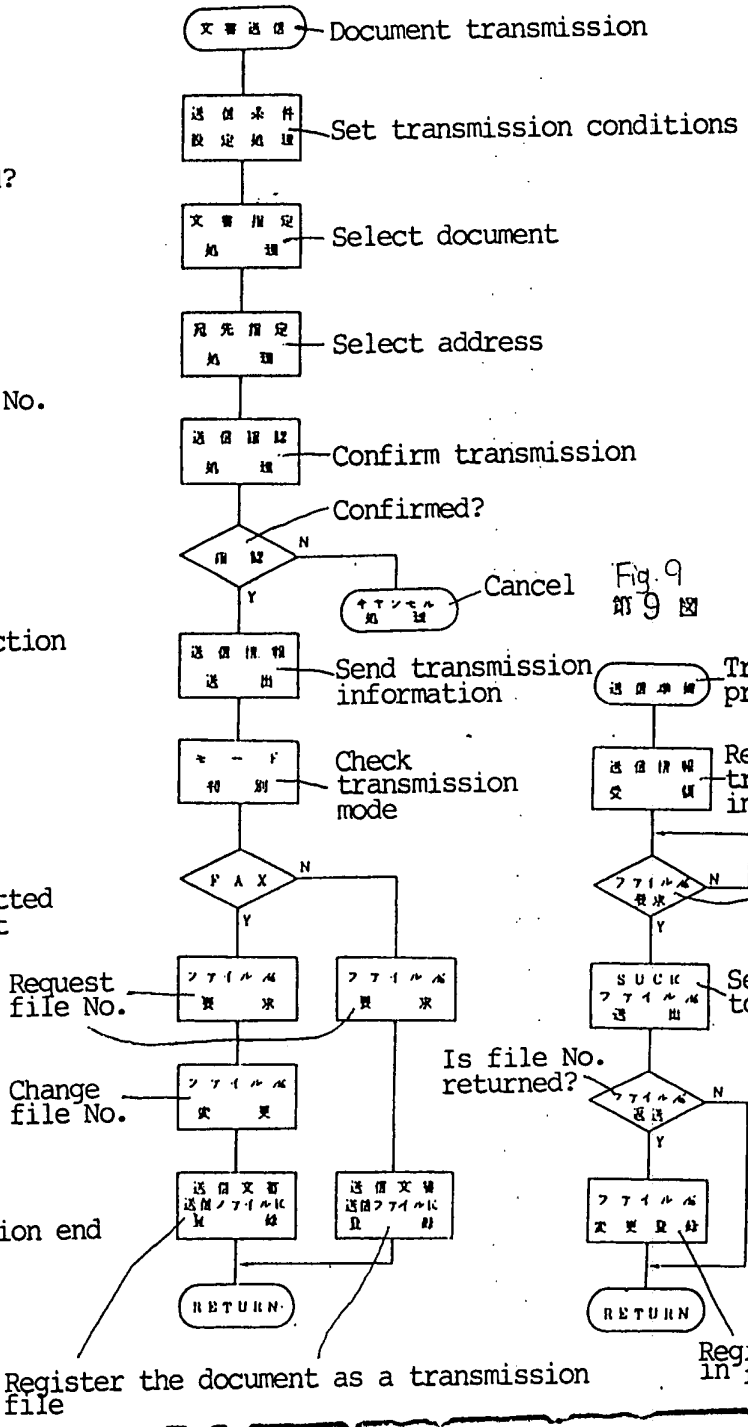
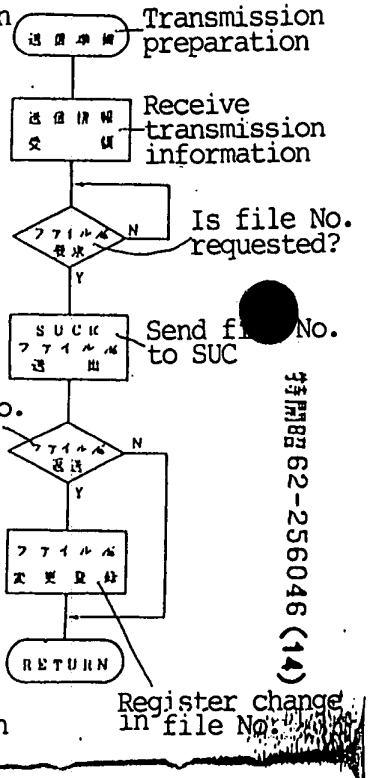


Fig. 9
第9図



特開昭62-256046 (14)

Fig. 13
第13図

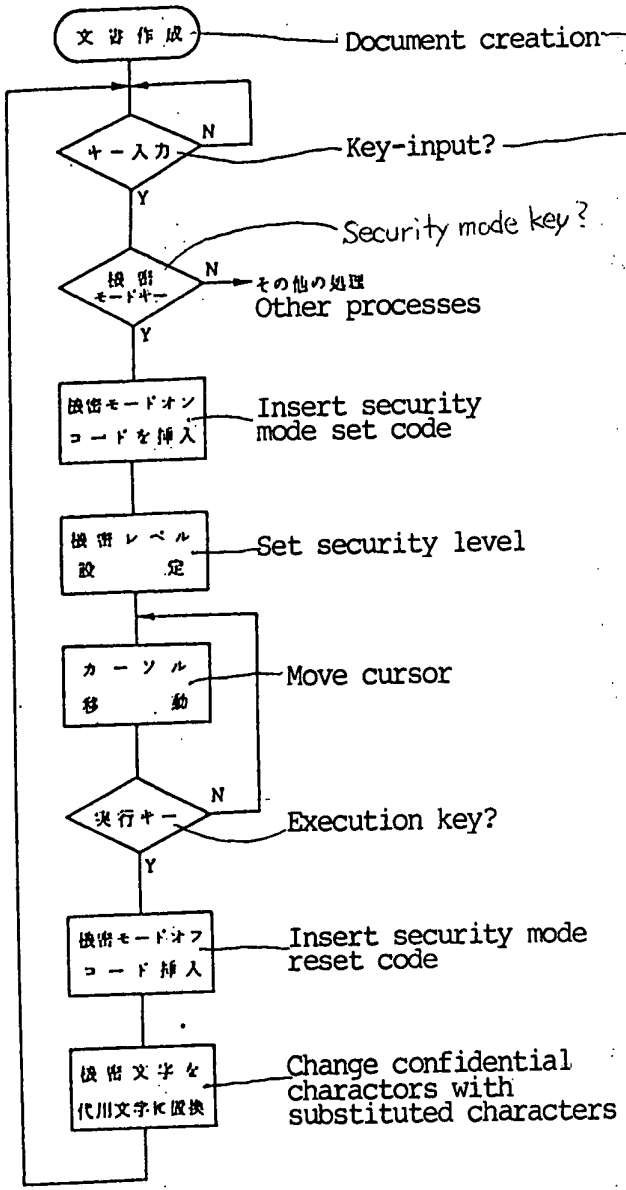
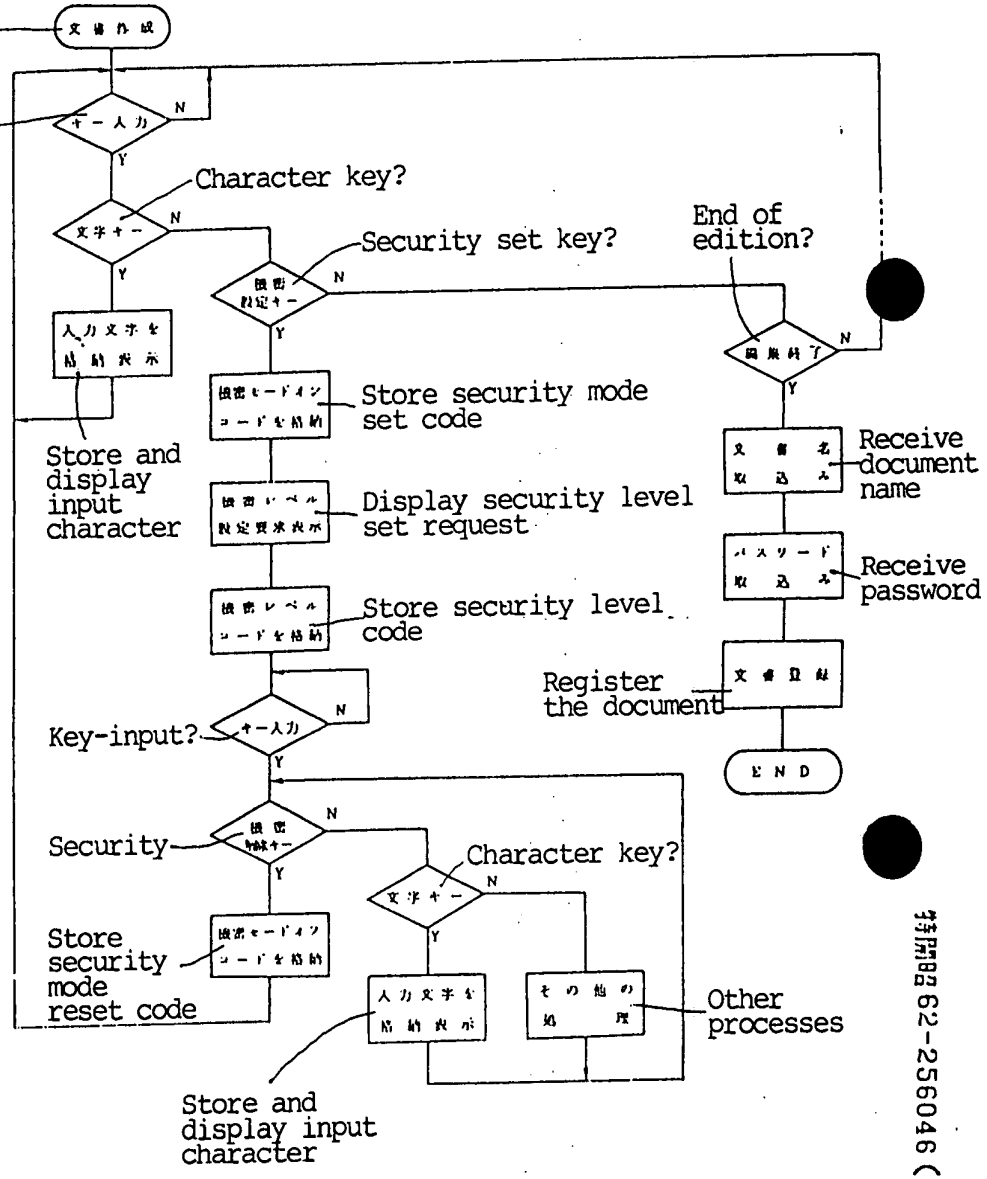


Fig. 12
第12図



特開昭62-256046(15)

第14図

(イ)

ＡＢＣ
機番：15
名称：DE
原価：100万

(ロ)

ＡＢＣ
機番：15
名称：DE
原価：[▨]万

第15図

原	価	:	モードON	文書レベル	1	0	0	モードOFF	万		

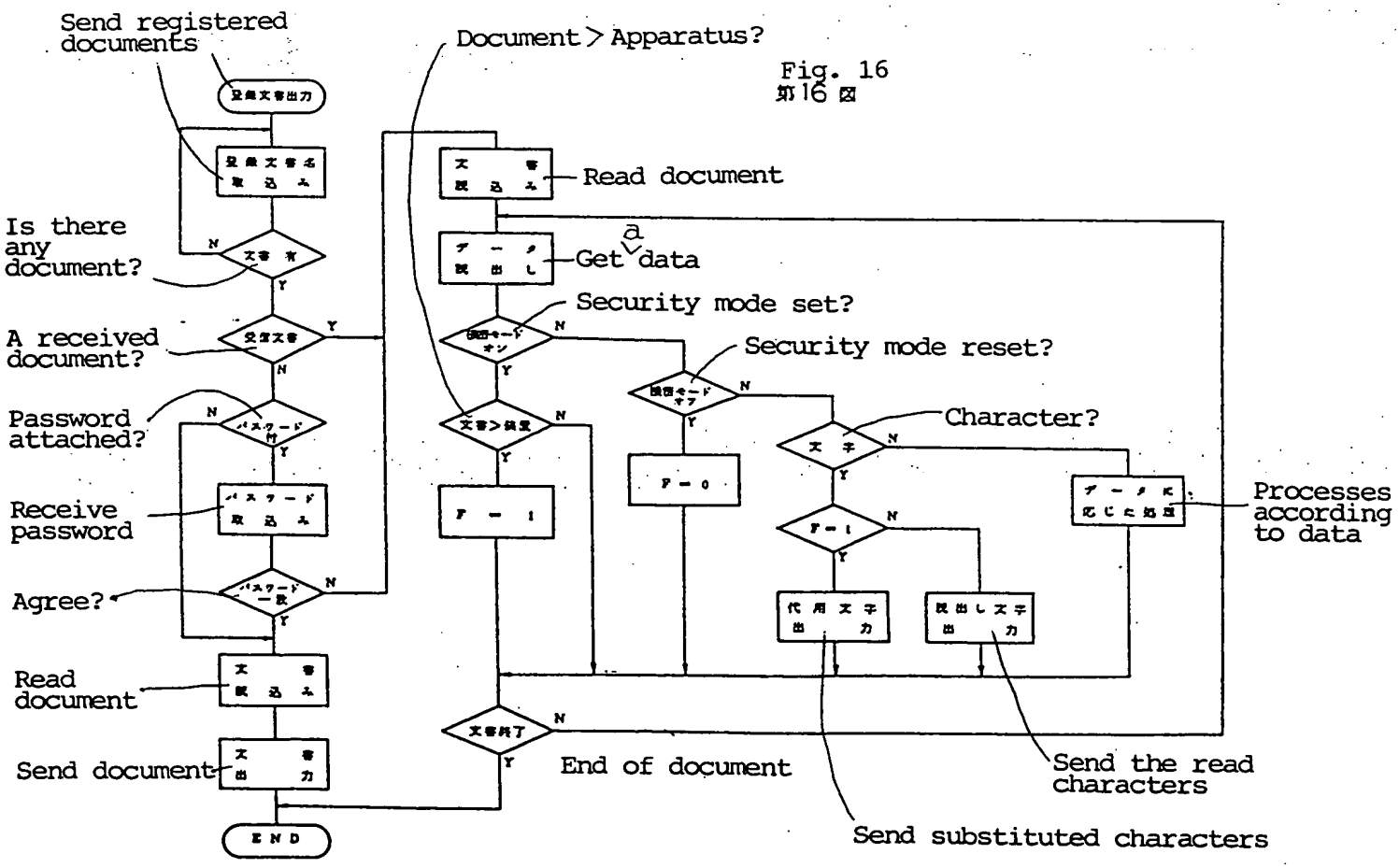


Fig. 16
第16図